SNB6500

EN User manual 3

PHILIPS

☎ Helpline

België/Belgique/Belgien
070 253 010 (€ 0.17)

Luxemburg/Luxembourg
26 84 30 00

Danmark
3525 8761

Deutschland
0180 5 007 532 (€ 0.12)

España
902 888 785 (€ 0.15)

France
08 9165 0006 (€ 0.23)

Ελλάδα
0 0800 3122 1223

Ireland
01 601 1161

Italia
199 404 042 (€ 0.25)

Cyprus
800 92256

Nederland
0900 0400 063 (€ 0.20)

Norge
2270 8250

Österreich
01 546 575 603 (low rate)

Portugal
2 1359 1440

Schweiz/Suisse/Svizzera
02 2310 2116

Suomi
09 2290 1908

Sverige
08 632 0016

Türkiye
0800 2613302

UK (United Kingdom)
0906 1010 017 (£ 0.15)

China 中国
4008 800 008

European Regulations

This product has been designed, tested and manufactured according to the European R&TTE Directive 1999/5/EC.

Following this Directive, this product can be brought into service in the following states:

SNB6500/00/05

B ✔	DK ✔	E ✔	GR ✔	F ✔
IRL ✔	I ✔	L ✔	NL ✔	A ✔
P ✔	SU ✔	S ✔	UK ✔	N ✔
D ✔	CH ✔			

Contents

EN

Contents **3**

Important safety information **4**

Safety Precautions 4

Environmental information 4

Disclaimer 4

What's in the box **5**

Introduction **6**

What are wireless network connections? 6

Factors determining your network range and network speed 6

Securing your wireless network 6

Your Wireless Router **7**

Install **8**

Securing your Home Network **13**

Firewall 13

Wireless encryption 14

Menu: Setup Wizard **22**

Menu: Home Network Settings **23**

Menu: Security Settings **25**

Menu: Advanced Settings **31**

Configure Client PC **35**

Finding the MAC address of a network card **41**

How to set-up a computer network **41**

Troubleshooting **47**

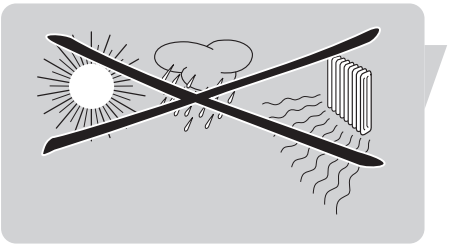
Glossary of terms **48**

Technical Specifications **49**

Important safety information

- Please install and connect the product in the order as described in the 'Quick Start Guide' booklet only. This assures best installation results with the least technical hassles.
- Please read this manual and the 'Quick Start Guide' booklet carefully before using the Wireless Router (SNB6500); and keep these documents for future reference.
- The most recent downloads and information on this product will be available through our web site www.philips.com/support
- During set-up and installation, it may be helpful to have the instructions for your PC and other network components at hand.

Safety Precautions



- Radio equipment for wireless applications is not protected against disturbance from other radio services.
- Do not expose the system to excessive moisture, rain, sand or heat sources.
- The product should not be exposed to dripping or splashing.
  No object filled with liquids, such as vases, should be placed on the product.
- Keep the product away from domestic heating equipment and direct sunlight.
- Allow a sufficient amount of free space all around the product for adequate ventilation.
- Do not open this product. Contact your Philips retailer if you experience technical difficulties.

Environmental information

All redundant packing material has been omitted. We have done our utmost to make the packaging easily separable into two mono materials: cardboard (box) and polyethylene (bags, protective foam sheet).Your set consists of materials that can be recycled if disassembled by a specialised company. Please observe the local regulations regarding the disposal of packing materials and old equipment.

Disclaimer

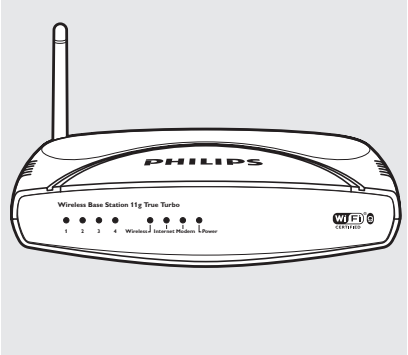
This product is provided by 'Philips' 'as is' and without any express or implied warranty of any kind of warranties, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed.

In no event shall Philips be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of information, data, or profits; or business interruption) howsoever caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of inability to use this product, even if advised of the possibility of such damages.

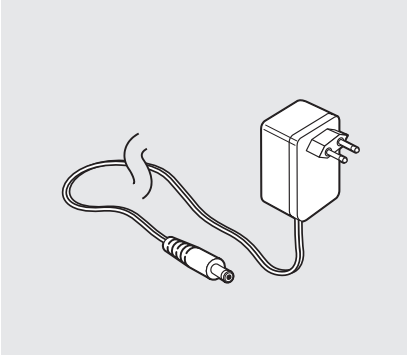
Philips further does not warrant the accuracy or completeness of the information, text, graphics, links or other items transmitted by this product.

What's in the box

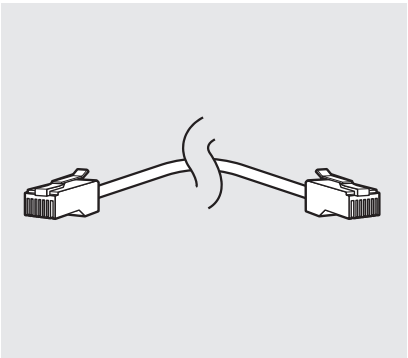
EN



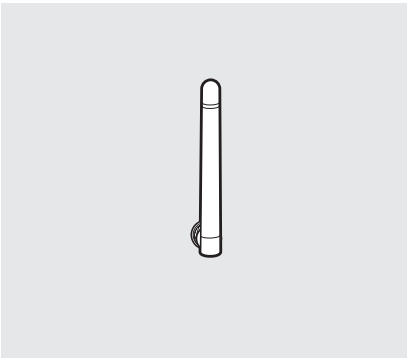
SNB6500



Power Supply



Ethernet Cable

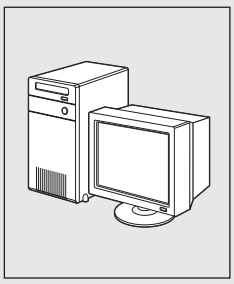


Antenna

Quick Start Guide

Installation CD

What else you will need



Computer

Broadband modem (cable modem or ADSL modem) with Ethernet port (Broadband modems with a USB connector are not supported)

Ethernet Network Card or Wi-Fi adapter

Introduction

SNB6500

Thank you for purchasing the Philips Wireless Router. This Philips Wireless Router is a WiFi (IEEE 802.11b/g) compatible device. It fully supports high data rates up to 108 Mbps with automatic fallback to lower speeds for secure operation at lower data rates in even the most difficult of wireless environments.

In this manual we will expand on how to install, configure, and use your Philips Wireless Router.

This chapter will give you background information on wireless networks and their security in general.

What are wireless network connections?

Your Wireless Router uses a wireless protocol (called IEEE 802.11b/g or WiFi) to communicate with other network computers by means of radio transmissions. WiFi radio waves travel outwards from the antenna in all directions, and can transmit through walls and floors. Wireless transmissions can theoretically reach up to 450 meters in an open environment and reach speeds of up to 108 Megabits per second (Mbps) at close range. However, the actual network range and data throughput rate will be less, depending on the wireless link quality.

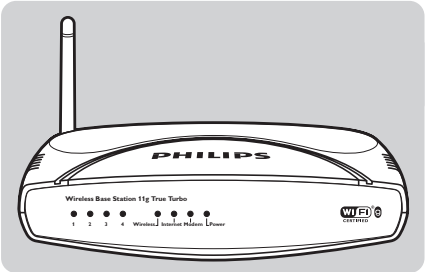
Factors determining your network range and network speed

- The environment: Radio signals can travel further outside of buildings, and if the wireless components are in direct line of sight to one another. Putting wireless components in high places helps avoid physical obstacles and provides better coverage.
- Building construction such as metal framing and concrete or masonry walls and floors will reduce radio signal strength. Avoid putting wireless components next to walls and other large, solid objects; or next to large metal objects such as computers, monitors, and appliances.
- Wireless signal range, speed, and strength can be affected by interference from neighbouring wireless networks and devices. Electro-magnetic devices such as televisions, radios, microwave ovens, and cordless phones, especially those with frequencies in the 2.4 GHz range, may also interfere with wireless transmission.
- Standing or sitting too close to wireless equipment can also affect radio signal quality.
- Adjusting the antenna: Do not place antennas next to large pieces of metal, because this might cause interference.

Securing your wireless network

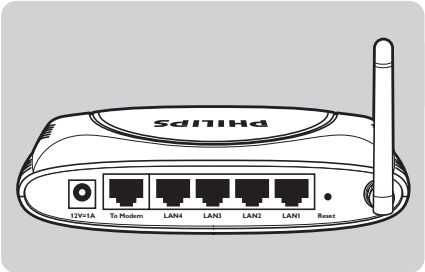
As wireless computer networks use radio signals, it is possible for other wireless network devices outside your immediate area to pick up the wireless signals and either connect to your network or to capture the network traffic.Therefore, you should always enable the Wired Equivalent Privacy **(WEP)** or WiFi Protected Access **(WPA/WPA2)** network encryption key to help prevent unauthorised connections or the possibility of eavesdroppers listening in on your network traffic.

For an example of how to secure your network, please see the chapter on **Securing your wireless network**.



Light	Status	Description
1 – 4	On	Ethernet connection is established
	Blinking	Send / Receive data
	Off	No cable connected
Wireless	On	Wireless Link is up
	Blinking	Send / Receive data
	Off	Wireless signal is disabled
Internet	On	Connected to Internet
	Blinking	Send / Receive data
	Off	No Internet connection
Modem	On	Connected to a Ethernet Broadband Modem
	Off	Not connected
Power	On	Power on, normal operation
	Off	Power off or failure

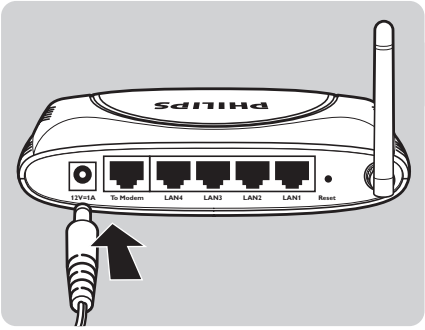
Image of rear side explaining ports and buttons



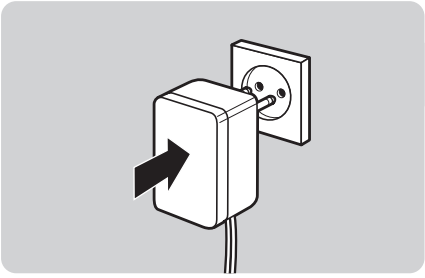
'9V⎓1A' port	Connect the included power adapter to this inlet.
'To Modem' port	Wide area Network port. Connect this to your broadband modem
LAN1 – LAN4 ports	10/100 Mbps Ethernet ports (RJ-45). Connect devices on your local area network to these ports (i.e. a PC, a Ethernet hub, or switch)
'Reset' button	Press this button for at least 5 seconds to reset the Wireless Router to its factory default settings. WARNING: THIS WILL DELETE YOUR INTERNET SETTINGS! To reset the Wireless Router without losing the configuration settings, see 'Reset' (see 'Menu Advanced Settings').

Powering up the Wireless Router and connecting the cables

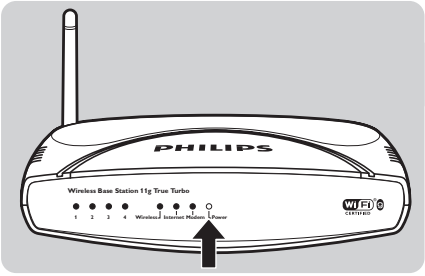
Connect power to the Wireless Router



Connect the supplied power adapter to the 9V⎓1A port.

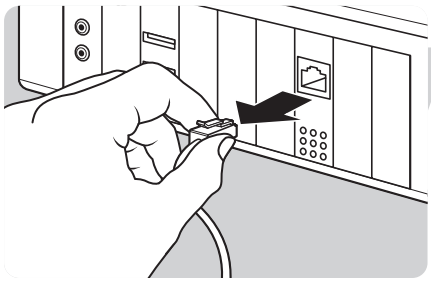


Connect Power Adapter to power socket.

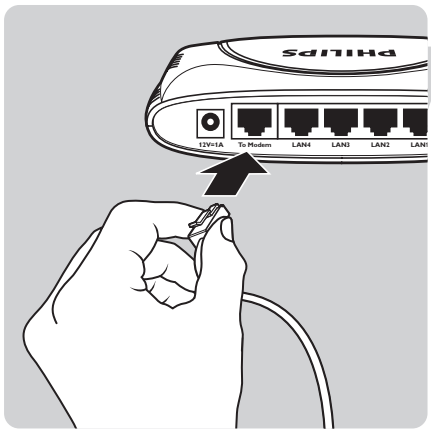


Power light will turn on.

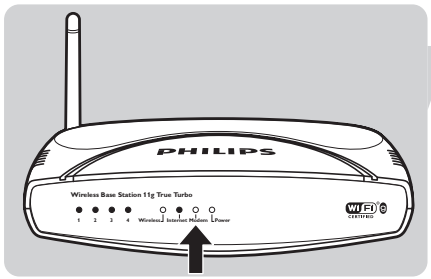
Connect Broadband Modem the Wireless Router



Disconnect Ethernet cable between PC and your broadband modem at the PC side.

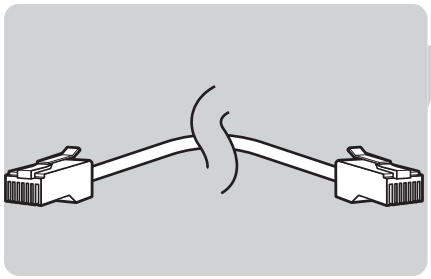


Connect the Ethernet cable to **To Modem** port.

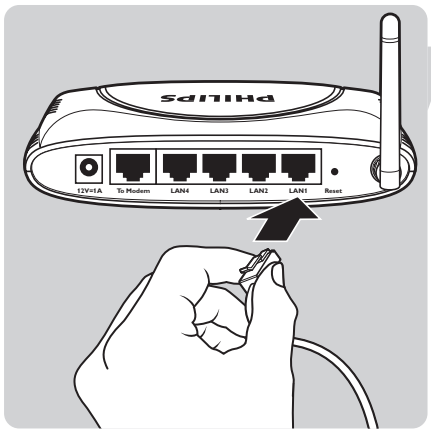


The **Modem** light will turn on.

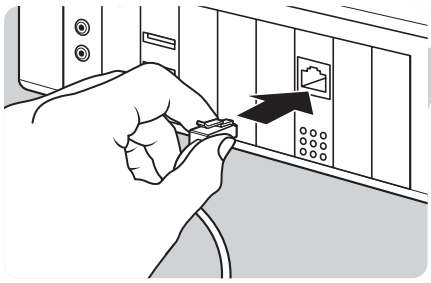
Connect PC to Wireless Router: Wired



Take the supplied Ethernet cable.

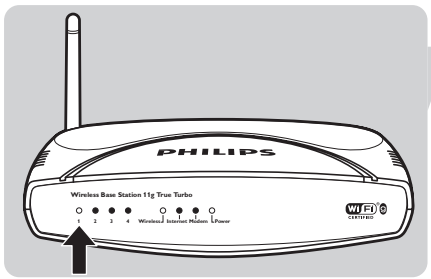


Connect one end of the Ethernet cable to **LAN1** port on SNB6500.



Connect other end of Ethernet cable to your PC network card.

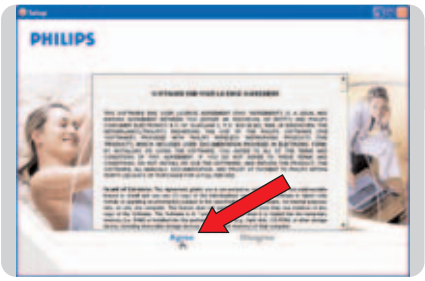
Network card must be configured to obtain an ip address automatically (see chapter "Configuring Client PC")



Light **1** on the front will turn on.

Configuring the Wireless Router with Installation CD

Place the installation CD in the CD-Drive.

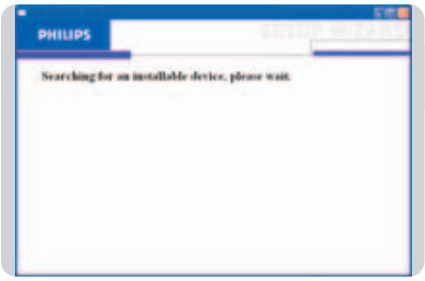


Select **Agree**.

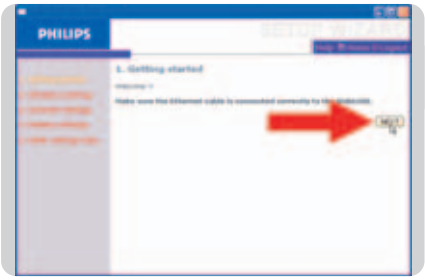
If this screen does not appear, start the CD manually
1 Open **My computer**
2 Open CD-Drive
3 Open Setup.exe

Select **SNB6500**.

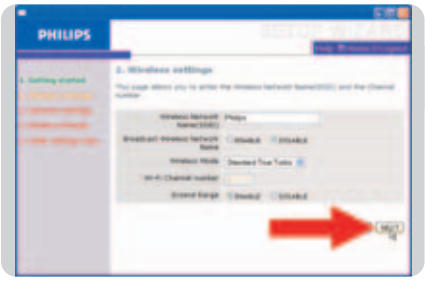
Click **Install Software**.



Wait until device (Wireless Router) is found.

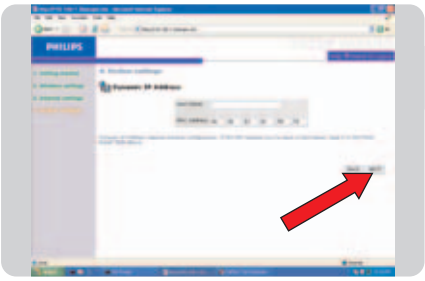


Click **Next**.



Click **Next**.

Select your Broadband modem type (DHCP).

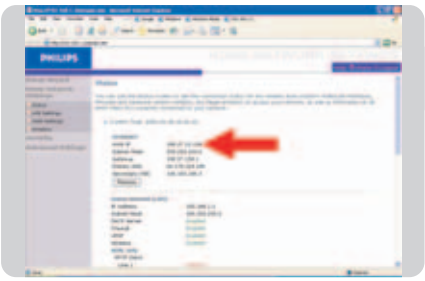


Enter your Broadband Settings.
These settings should be provided to you by your ISP.

(this example shows the cable modem configuration)

Wait until your settings have been saved.

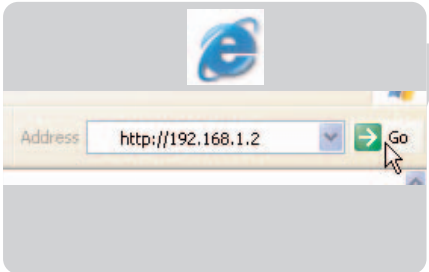
Click **LOGIN** (Enter password if set).



The status window will show you are connected to the Internet.

Firewall

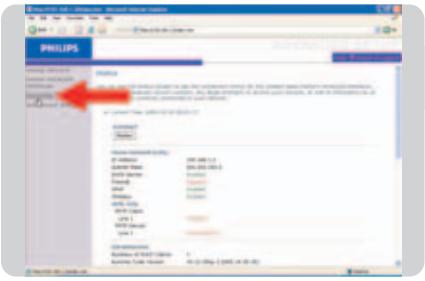
Enable the Firewall to protect your Home Network against hackers.



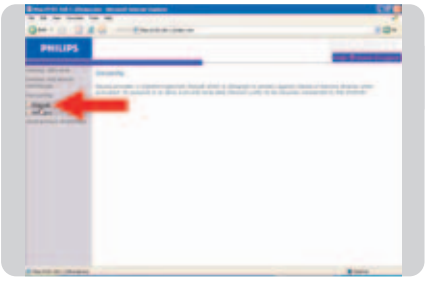
Open your Internet browser.

1. Enter http://192.168.1.2 in the address bar.
2. Click **Go**.

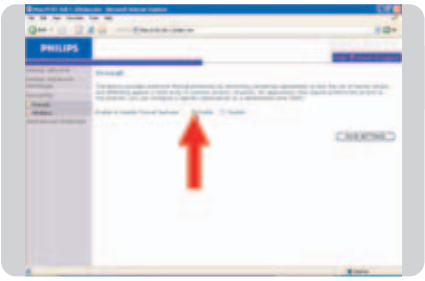
Click **LOGIN** (Enter password if set).



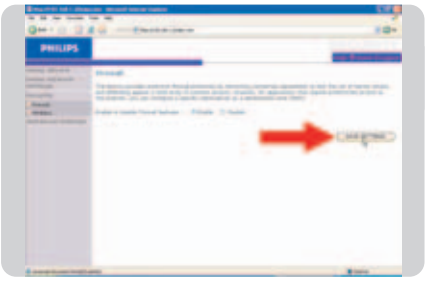
Click **Security**.



Click **Firewall**.



Select **Enable**.



Click **SAVE SETTINGS**.

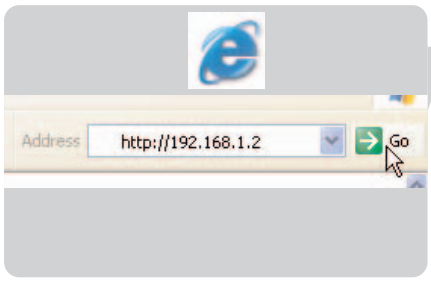
Wireless encryption

Enable Wireless Encryption to prevent others from eavesdropping your wireless connection.

Wi-Fi Protected Access (WPA/WPA2)

Step 1: Setup the WPA/WPA2 encryption

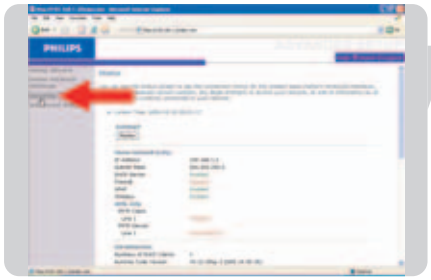
Step 1



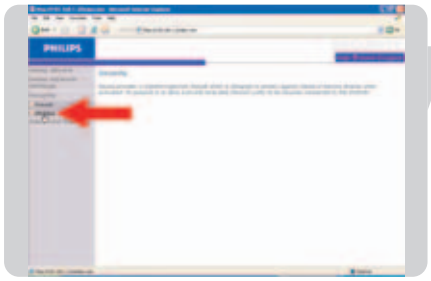
Open your Internet browser

1. Enter http://192.168.1.2 in the address bar.
2. Click **Go**.

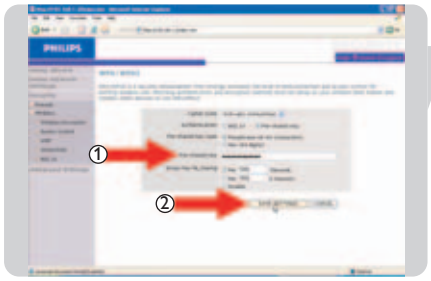
Click **LOGIN** (Enter password if set).



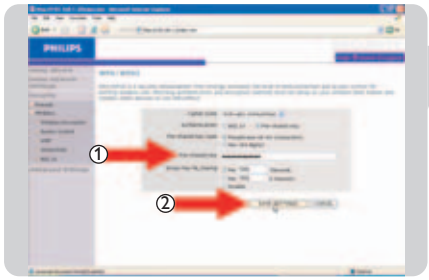
Click **Security**.



Click **Wireless**.



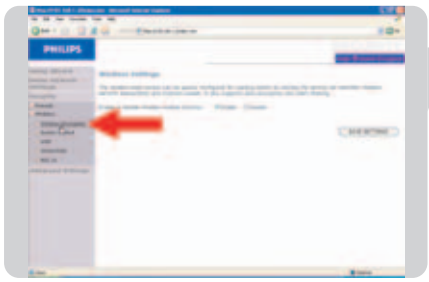
Select **WPA&WPA2**.



1 Enter your Pre-shared Key (= password or passphrase)
2 Click **SAVE SETTINGS**.

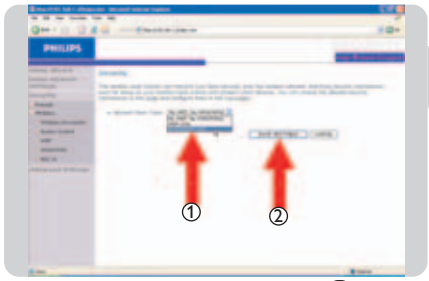
WARNING: WPA/WPA2 encryption is still not active at this point

Step 2



Step 2: Enable WPA/WPA2 Encryption.

Click **Wireless Encryption**.



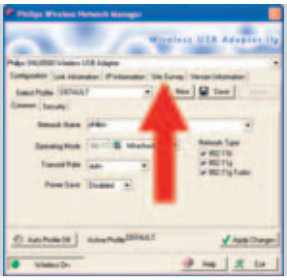
1. Select **WPA/WPA2 Only**
2 Click **SAVE SETTINGS**.

WPA/WPA2 encryption is now active.

Step 3

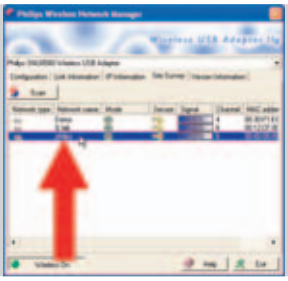
Step 3: Connect to the Wireless Router
This example shows how to connect using the Philips Wireless USB Adapter (SNU6600)

Double click the **Philips Wireless USB Adapter 11g** desktop Icon.

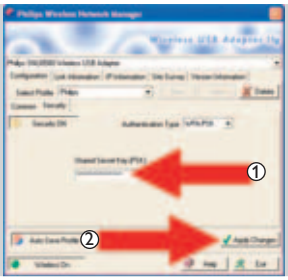


1 Select **Site Survey**.
2 Click **Scan**.

Click **Scan**.



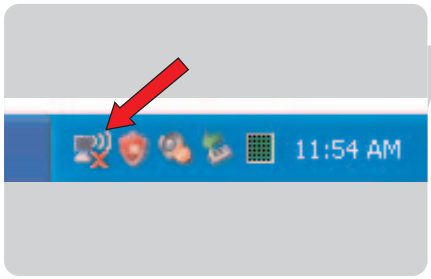
Double click your encrypted Wireless Router.



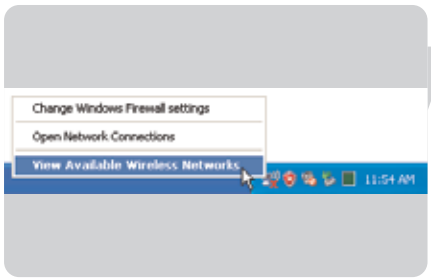
1. Enter the Pre-Shared Key.
2. Click **Apply Changes**.

Check **IP Information**.
Gateway should be 192.168.1.2

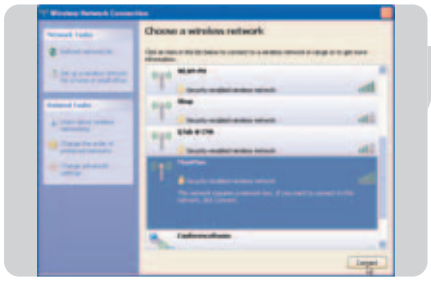
This example shows screenshots of the Windows XP Wireless Network Connection



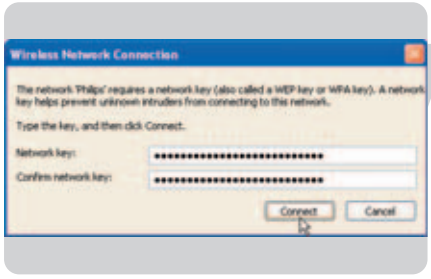
Move mouse to System tray Wireless Icon.



Right mouse click on Wireless Icon.
Click **View available Wireless Networks**.



Click your encrypted Wireless Router.
Click **Connect**.



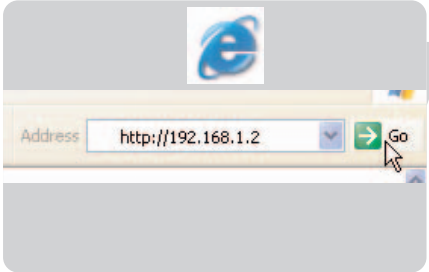
Enter WPA/WPA2 Pre-Shared Key (Network Key in Windows XP terminology).
Click **Connect**.

You are now succesfully connected.

Wired Equivalent Privacy (WEP)

Step 1

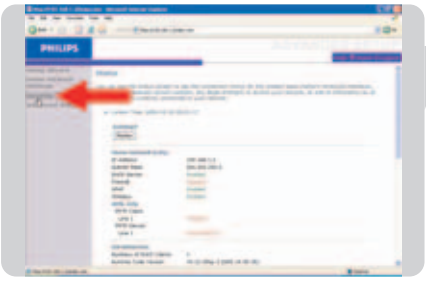
Step 1: Setup the WEP encryption



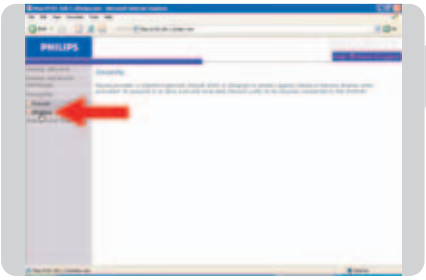
Open your Internet browser

1. Enter http://192.168.1.2 in the address bar.
2. Click **Go**.

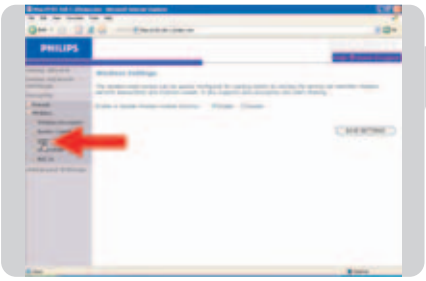
Click **LOGIN** (Enter password if set).



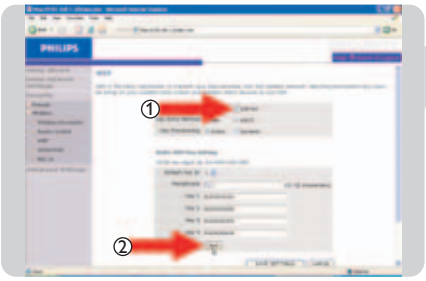
Click **Security**.



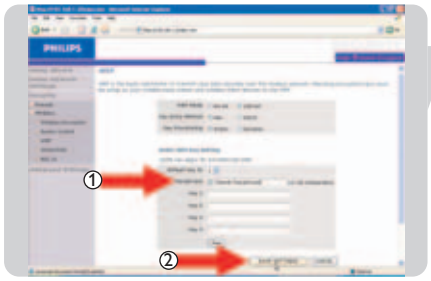
Click **Wireless**.



Click **WEP**.

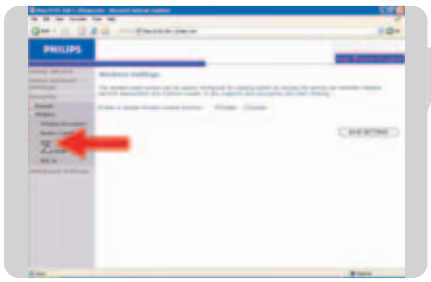


1 Select **128-bit**.
2 Click **Clear**.

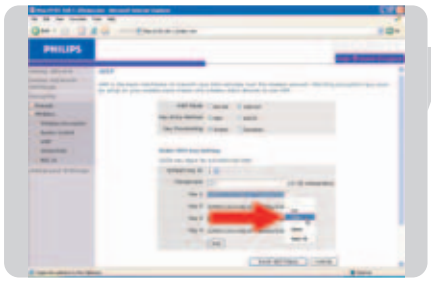


1 Checkmark the 'Passphrase' box and enter the passphrase.
2 Click **SAVE SETTINGS**.

WARNING: WEP encryption is still not active at this point



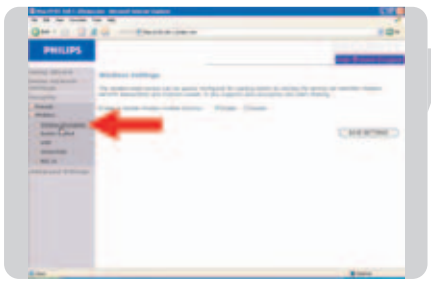
Click **WEP**.



Copy the WEP encryption key.
Double click Key1. Right mouse click. Click copy.

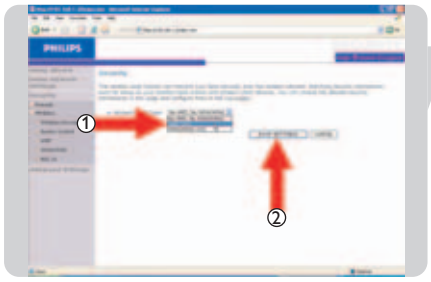
Save this key for later use.

Step 2



Step 2: Enable WEP Encryption

Click **Wireless Encryption**.



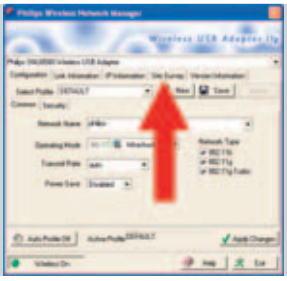
1 Select **WEP Only**.
2 Click **SAVE SETTINGS**.

WPA/WPA2 encryption is now active.

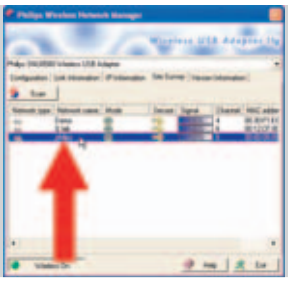
Step 3

Step 3: Connect to the Wireless Router.
This example shows screenshots of the Philips Wireless USB Adapter (SNU6600)

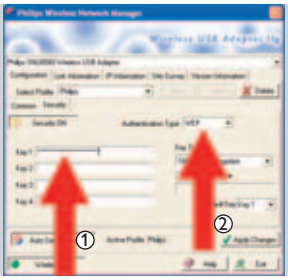
Double click the **Philips Wireless USB Adapter 11g** desktop Icon.



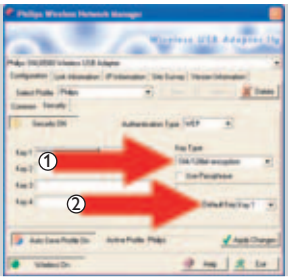
1 Select **Site Survey**.
2 Click **Scan**.



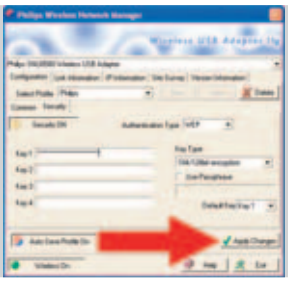
Double click your encryptyed Wireless Router.



1 Select Authentication Type **WEP**.
2 Enter WEP key copied from your Wireless Router.



1 Select Key Type **104/128 bit Encryption**.
2 Enter Default Key **Key 1**.



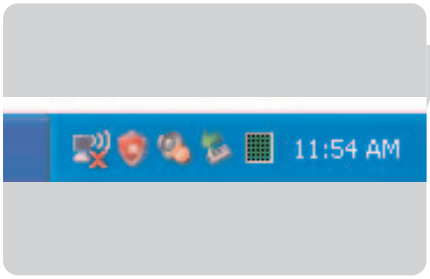
Click **Apply Changes**.

Check Gateway IP status

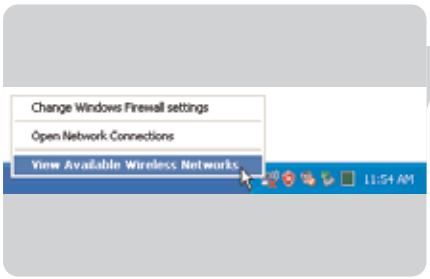
Gateway should be 192.168.1.2

Step 3

Step3: Connect to the Wireless Router
This example shows how to connect to the Wireless Router using Windows XP.



Move mouse to System tray Wireless Icon



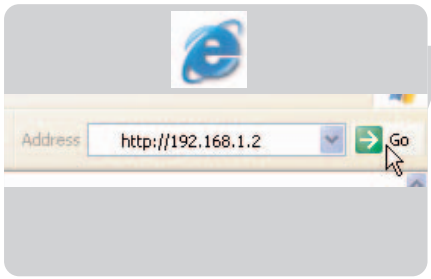
Right mouse click on Wireless Icon.
Click **View available Wireless Networks**.

Click your encrypted Wireless Router.
Click **Connect**.

Enter WEP
(Network Key in Windows XP terminology)
Click **Connect**.

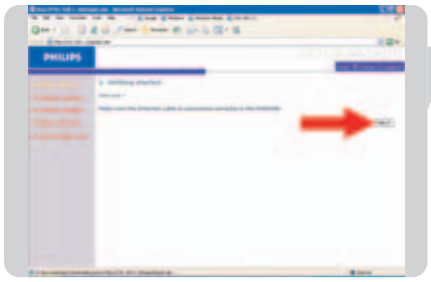
You are now successfully connected

Menu: Setup Wizard

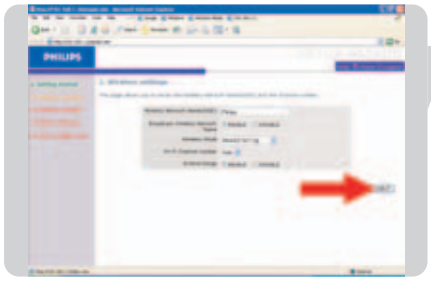


Open your Internet browser

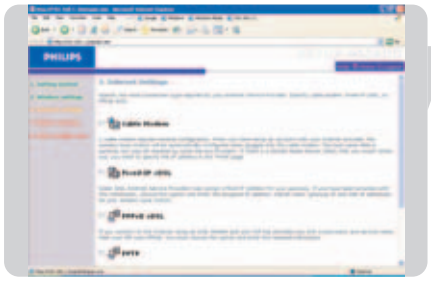
1. Enter http://192.168.1.2 in the address bar
2. Click **Go**.



Click **NEXT**.

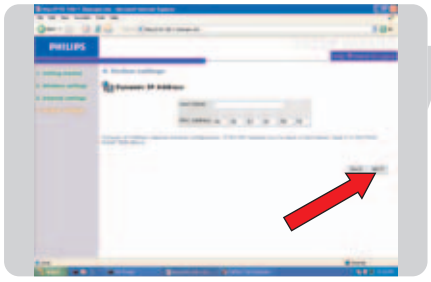


Click **NEXT**.

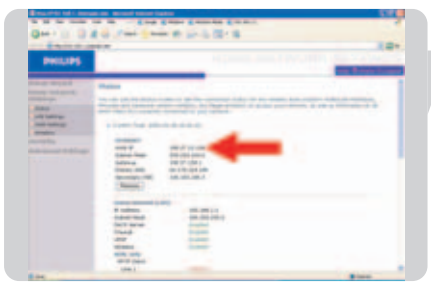


Select your Internet Settings.

The type of broadband internet connection you have is described in the documentation of your ISP.



Enter you ISP settings (Dynamic IP Address in this example).
Click **NEXT**.



The Status shows ISP IP address.

Home network settings

Status
The Status page displays WAN/LAN connection status, firmware, and hardware version numbers, illegal attempts to access your network, as well as information on DHCP clients connected to your network. The security log may be saved to a file by clicking 'Save' and choosing a location.

Network settings
Use the Home Networking menu to configure the LAN IP address and to enable the DHCP server for dynamic client address allocation.

Note: *Remember to configure your client PCs for dynamic IP address allocation.*

Wireless
The Wireless Router also operates as a wireless access point, allowing wireless computers to communicate with each other. To configure this function, you need to enable the wireless function, define the radio channel, the domain identifier, and the security options.
Check Enable and click 'SAVE SETTINGS'.

Channel and SSID
You must specify a common radio channel and SSID (Service Set ID) to be used by the Wireless Router and all of its wireless clients.
Make sure you configure all of its clients to the same values.

Access Control
Access Control allows users to define the outgoing traffic permitted or not-permitted through the WAN interface. The default is to permit all outgoing traffic.

To add the PC to the filtering table:

1 Click 'Add PC' on the Access Control screen.

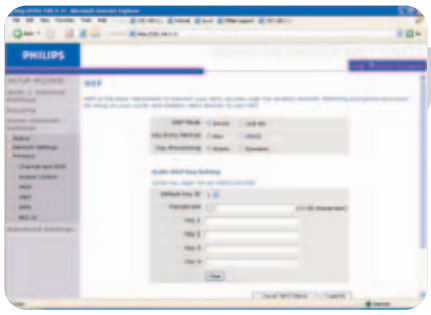
2 Define the appropriate settings for client PC services.

3 Click 'OK' and then click 'SAVE SETTINGS' to save your settings.

WDS
If the signal strength of a single Wireless Router is not sufficient due to a large coverage area or attenuation due to walls, with WDS the range of a Wireless Router can be extended.

All Routers in a Wireless Distribution System must be configured with the same radio channel, and encryption type (WEP / WPA/WPA2) if that is used.

Note: *The WDS feature is not completely specified in IEEE or Wifi standards. Therefore it cannot be guaranteed that WDS will work with products of different vendors.*

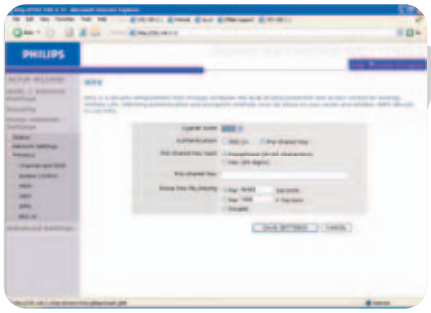


WEP
If you use WEP to protect your wireless network, you need to set the same parameters for the Wireless Router and all your wireless clients.

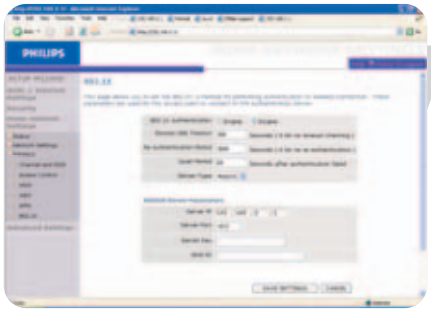
You may automatically generate encryption keys or manually enter the keys. To generate the key automatically with passphrase, check the Passphrase box, enter a string of characters. Select the default key from the drop down menu. Click 'SAVE SETTINGS'.

Note: *The passphrase can consist of up to 32 alphanumeric characters.*

To manually configure the encryption key, enter five hexadecimal pairs of digits for each 64-bit key, or enter 13 pairs for the single 128-bit key.
(A hexadecimal digit is a number or letter in the range 0-9 or A-F.)
Note that WEP protects data transmitted between wireless nodes, but does not protect any transmissions over your wired network or over the Internet.



WPA/WPA2
Wi-Fi Protected Access (WPA/WPA2) combines temporal key integrity protocol (TKIP) and 802.1x mechanisms. It provides dynamic key encryption and 802.1x authentication service.



802.1X
If 802.1x is used in your network, then you should enable this function for the Wireless Router. These parameters are used for the Wireless Router to connect to the authentication server.

Security

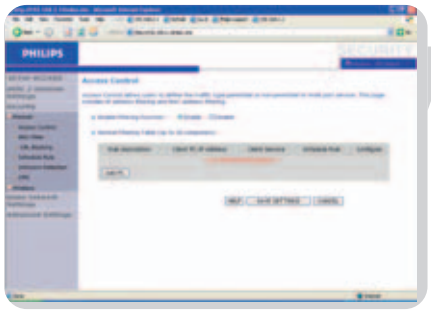
Firewall

The Wireless Router's firewall inspects packets at the application layer, maintains TCP and UDP session information including time-outs and the number of active sessions, and provides the ability to detect and prevent certain types of network attacks.

Network attacks that deny access to a network device are called Denial-of-Service (DoS) attacks. DoS attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources.

The Wireless Router firewall function protects against the following DoS attacks: IP Spoofing, Land Attack, Ping of Death, IP with zero length, Smurf Attack, UDP port loopback, Snork Attack, TCP null scan, and TCP SYN flooding.

The firewall does not significantly affect system performance, so we advise leaving it enabled to protect your network. Select Enable and click the 'SAVE SETTINGS' button to open the Firewall submenus.



Access Control

Access Control allows users to define the outgoing traffic permitted or not-permitted through the WAN interface. The default is to permit all outgoing traffic.

To add the PC to the filtering table:

1 Click 'Add PC' on the Access Control screen.

2 Define the appropriate settings for client PC services.

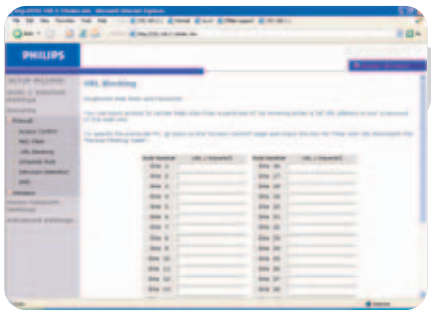
3 Click 'OK' and then click 'SAVE SETTINGS' to save your settings.

MAC Filter

The Wireless Router can also limit the network access based on the MAC address. The MAC Filtering Table allows the Wireless Router to enter up to 32 MAC addresses that are not allowed access to the WAN port.

1 Click Yes to enable, or No to disable this function.

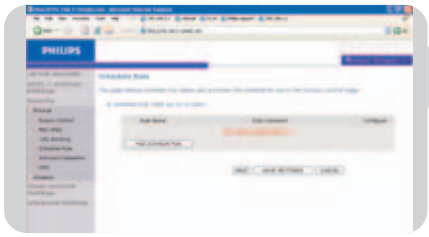
2 Enter the MAC address in the space provided and click 'Save Settings' to confirm.



URL Blocking

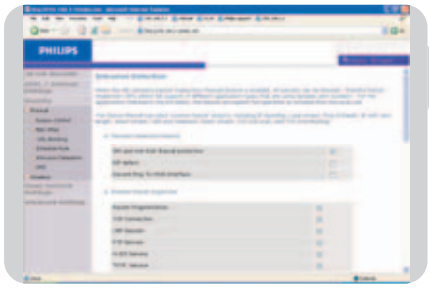
The Wireless Router allows the user to block access to web sites by entering either a full URL address or just a keyword. This feature can be used to protect children from accessing violent or pornographic web sites.

You can define up to 30 sites here.



Schedule Rule
You may filter Internet access for local clients based on rules. Each access control rule may be activated at a scheduled time. Define the time schedule on this page, and apply the rule on the Access Control page.

Intrusion Detection



Intrusion Detection Feature
Stateful Packet Inspection (SPI) and Anti-DoS firewall protection (Default: Enabled) - The Intrusion Detection Feature of the Wireless Router limits access for incoming traffic at the WAN port. When the SPI feature is turned on, all incoming packets will be blocked except for those types marked in the Stateful Packet Inspection section.

RIP Defect (Default: Disabled) - If an RIP request packet is not acknowledged to by the router, it will stay in the input queue and not be released. Accumulated packets could cause the input queue to fill, causing severe problems for all protocols. Enabling this feature prevents the packets from accumulating.

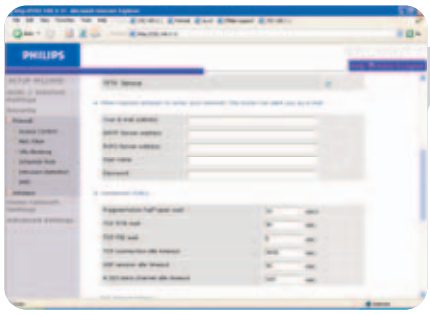
Discard Ping to WAN (Default: Disabled) - Prevent a ping on the Wireless Router's WAN port from being routed to the network.

Scroll down to view more information.

Stateful Packet Inspection
This is called a 'stateful' packet inspection because it examines the contents of the packet to determine the state of the communications; i.e., it ensures that the stated destination computer has previously requested the current communication. This is a way of ensuring that all communications are initiated by the recipient computer and are taking place only with sources that are known and trusted from previous interactions. In addition to being more rigorous in their inspection of packets, stateful inspection firewalls also close off ports until connection to the specific port is requested.

When particular types of traffic are checked, only the particular type of traffic initiated from the internal LAN will be allowed. For example, if the user only checks 'FTP Service' in the Stateful Packet Inspection section, all incoming traffic will be blocked except for FTP connections initiated from the local LAN.

Stateful Packet Inspection allows you to select different application types that are using dynamic port numbers. If you wish to use the Stateful Packet Inspection (SPI) to block packets, click on the Yes radio button in the 'Enable SPI and Anti-DoS firewall protection' field and then check the inspection type that you need, such as Packet Fragmentation, TCP Connection, UDP Session, FTP Service, H.323 Service, or TFTP Service.



When hackers attempt to enter your network, the SNB6500 can alert you by e-mail

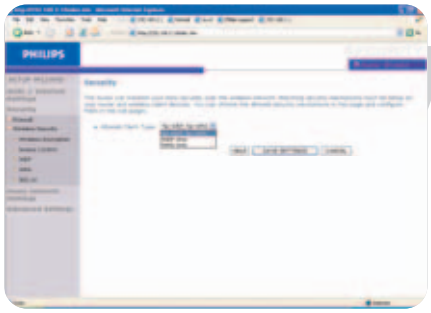
If the mail server needs to authenticate your identification before sending out any e-mail, please fill related information in POP3 server, username and password fields. Otherwise leave the three fields blank.

Connection Policy
Enter the appropriate values for TCP/UDP sessions as described in the following table.

Note: *The firewall does not significantly affect system performance, so we advise enabling the prevention features to protect your network.*

DMZ
If you have a client PC that cannot run an Internet application properly from behind the firewall, you can open the client up to unrestricted two-way Internet access. Enter the IP address of a DMZ (Demilitarized Zone) host on this screen. Adding a client to the DMZ may expose your local network to a variety of security risks, so only use this option as a last resort.

Wireless security



Wireless Encryption
To make your wireless network safe, you should turn on the security function.
The Wireless Router supports WEP (Wired Equivalent Privacy),
WPA/WPA2 (Wi-Fi Protected Access), and 802.1x security mechanisms.

Access Control
Access Control allows users to define the outgoing traffic permitted or not-permitted through the WAN interface. The default is to permit all outgoing traffic.

To add the PC to the filtering table:

1 Click 'Add PC' on the Access Control screen.

2 Define the appropriate settings for client PC services.

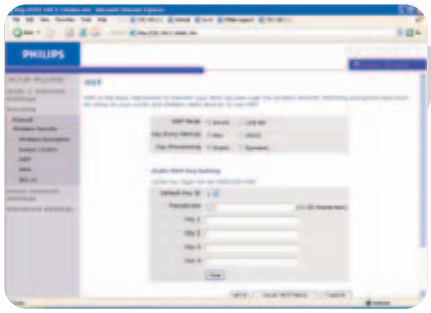
3 Click 'OK' and then click 'SAVE SETTINGS' to save your settings.

MAC Filter
The Wireless Router can also limit the network access based on the MAC address. The MAC Filtering Table allows the Wireless Router to enter up to 32 MAC addresses that are not allowed access to the WAN port.

1 Click Yes to enable, or No to disable this function.

2 Enter the MAC address in the space provided and click 'Save Settings' to confirm.

Note: *Also see 'Finding the MAC address of a network card'.*



WEP
If you use WEP to protect your wireless network, you need to set the same parameters for the Wireless Router and all your wireless clients.

You may automatically generate encryption keys or manually enter the keys.
To generate the key automatically with passphrase, check the Passphrase box, enter a string of characters. Select the default key from the drop down menu.
Click 'SAVE SETTINGS'.

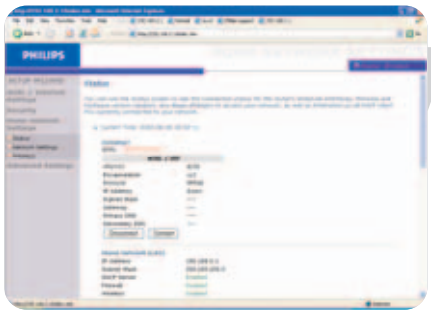
Note: *The passphrase can consist of up to 32 alphanumeric characters.*

To manually configure the encryption key, enter five hexadecimal pairs of digits for each 64-bit key, or enter 13 pairs for the single 128-bit key.
(A hexadecimal digit is a number or letter in the range 0-9 or A-F.)
Note that WEP protects data transmitted between wireless nodes, but does not protect any transmissions over your wired network or over the Internet.

WPA/WPA2
Wi-Fi Protected Access (WPA/WPA2) combines Temporal Key Integrity Protocol (TKIP) and 802.1x mechanisms. It provides dynamic key encryption and 802.1x authentication service.

802.1X
If 802.1x is used in your network, then you should enable this function for the Wireless Router. These parameters are used for the Wireless Router to connect to the authentication server.

Home network settings



Status
The Status page displays WAN/LAN connection status, firmware, and hardware version numbers, illegal attempts to access your network, as well as information on DHCP clients connected to your network. The security log may be saved to a file by clicking 'Save' and choosing a location.

Network settings
Use the Home Networking menu to configure the LAN IP address and to enable the DHCP server for dynamic client address allocation.

Note: *Remember to configure your client PCs for dynamic IP address allocation.*

Wireless
The Wireless Router also operates as a wireless access point, allowing wireless computers to communicate with each other. To configure this function, you need to enable the wireless function, define the radio channel, the domain identifier, and the security options.
Check Enable and click 'SAVE SETTINGS'.

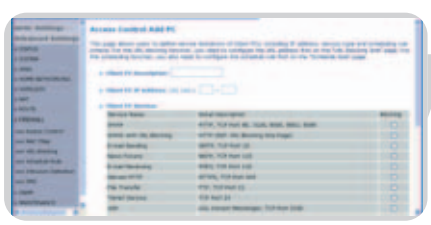
Channel and SSID
You must specify a common radio channel and SSID (Service Set ID) to be used by the Wireless Router and all of its wireless clients.
Make sure you configure all of its clients to the same values.

Access Control
Access Control allows users to define the outgoing traffic permitted or not-permitted through the WAN interface. The default is to permit all outgoing traffic.

To add the PC to the filtering table:

1 Click 'Add PC' on the Access Control screen.

2 Define the appropriate settings for client PC services.

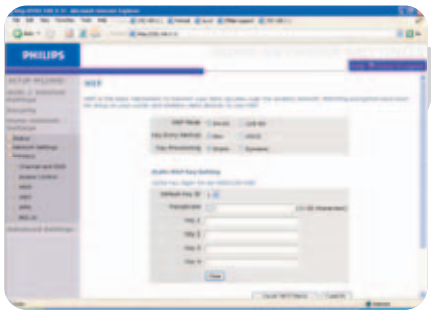


3 Click 'OK' and then click 'SAVE SETTINGS' to save your settings.

WDS
If the signal strength of a single Wireless Router is not sufficient due to a large coverage area or attenuation due to walls, with WDS the range of a Wireless Router can be extended.

All Routers and wireless range extenders (i.e. SNR 6500) in a Wireless Distribution System must be configured with the same radio channel, and encryption type (WEP / WPA/WPA2) if that is used.

Note: *The WDS feature is not completely specified in IEEE or Wifi standards. Therefore it cannot be guaranteed that WDS will work with products of different vendors.*

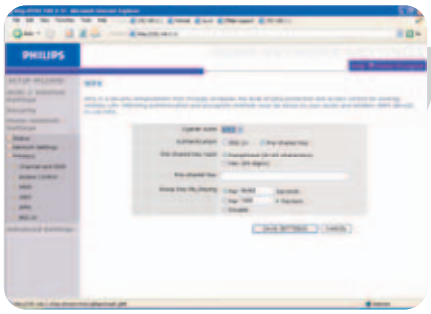


WEP
If you use WEP to protect your wireless network, you need to set the same parameters for the Wireless Router and all your wireless clients.

You may automatically generate encryption keys or manually enter the keys.
To generate the key automatically with passphrase, check the Passphrase box, enter a string of characters. Select the default key from the drop down menu. Click 'SAVE SETTINGS'.

Note: *The passphrase can consist of up to 32 alphanumeric characters.*

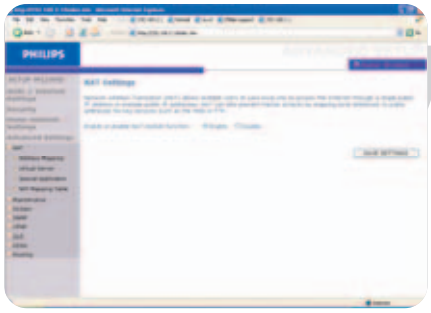
To manually configure the encryption key, enter five hexadecimal pairs of digits for each 64-bit key, or enter 13 pairs for the single 128-bit key.
(A hexadecimal digit is a number or letter in the range 0-9 or A-F.)
Note that WEP protects data transmitted between wireless nodes, but does not protect any transmissions over your wired network or over the Internet.



WPA/WPA2
Wi-Fi Protected Access (WPA/WPA2) combines Temporal Key Integrity Protocol (TKIP) and 802.1x mechanisms. It provides dynamic key encryption and 802.1x authentication service.

802.1X
If 802.1x is used in your network, then you should enable this function for the Wireless Router. These parameters are used for the Wireless Router to connect to the authentication server.

Advanced settings

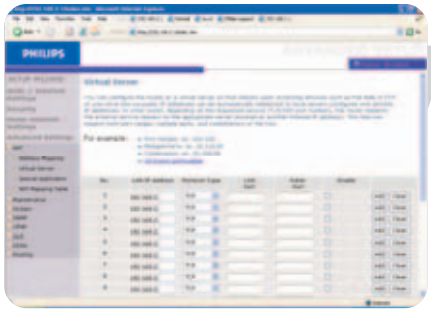


NAT

Network Address Translation allows multiple users to access the Internet sharing one public IP.

Address Mapping

Allows one or more public IP addresses to be shared by multiple internal users. This also hides the internal network for increased privacy and security. Enter the Public IP address you wish to share into the Global IP field. Enter a range of internal IPs that will share the global IP into the 'from' field.

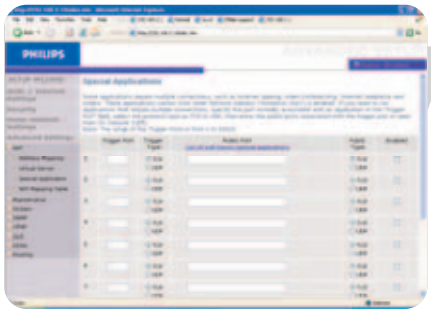


Virtual Server

If you configure the Wireless Router as a virtual server, remote users accessing services such as web or FTP at your local site via public IP addresses can be automatically redirected to local servers configured with private IP addresses. In other words, depending on the requested service (TCP/UDP port number), the Wireless Router redirects the external service request to the appropriate server (located at another internal IP address).

For example, if you set Type/Public Port to TCP/80 (HTTP or web) and the Private IP/Port to 192.168.1.10/80, then all HTTP requests from outside users will be transferred to 192.168.1.10 on port 80. Therefore, by just entering the IP address provided by the ISP, Internet users can access the service they need at the local address to which you redirect them.

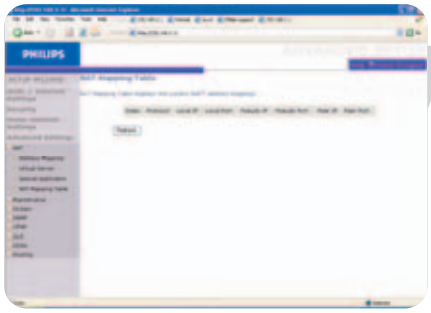
A list of ports is maintained at the following link:
http://www.iana.org/assignments/port-numbers.



Special Applications

Some applications require multiple connections, such as Internet gaming, video-conferencing, and Internet telephony.

These applications may not work when Network Address Translation (NAT) is enabled. If you need to run applications that require multiple connections, use these pages to specify the additional public ports to be opened for each application.



NAT Mapping Table

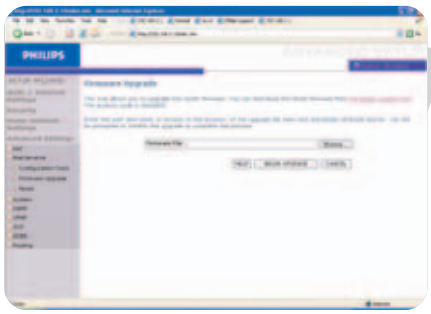
This page displays the current NAPT (Network Address Port Translation) address mappings.

Maintenance

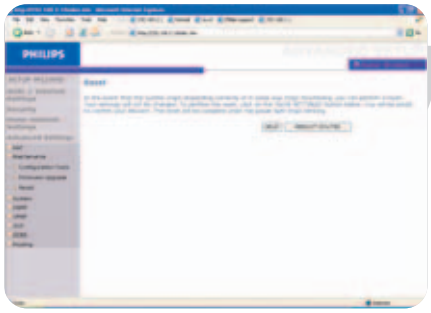
Use the Maintenance menu to backup the current configuration, restore a previously saved configuration, restore factory settings, update firmware, and reset the Wireless Router.

Configuration Tools
Choose a function and click Next.

Backup allows you to save the Wireless Router's configuration to a file. Restore can be used to restore the saved backup configuration file. Restore to Factory Defaults resets the Wireless Router to the original settings.
You will be asked to confirm your decision.



Firmware Upgrade
Use the Firmware Upgrade screen to update the firmware or user interface to the latest versions. Download the upgrade file from www.philips.com/support (Model SNB6500), and save it to your hard drive. Then click 'Browse...' to look for the downloaded file. Click 'BEGIN UPGRADE'. Check the Status page Information section to confirm that the upgrade process was successful.

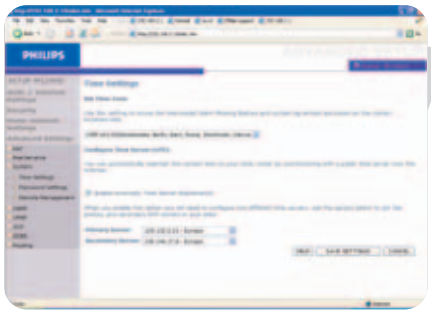


Reset
Click 'REBOOT ROUTER' to reset the Wireless Router.

If you perform a reset from this page, the configurations will not be changed back to the factory default settings.

Note: *If you use the Reset button on the rear panel, the Wireless Router performs a power reset. Press the button for over five seconds, and the factory default settings will be restored.*

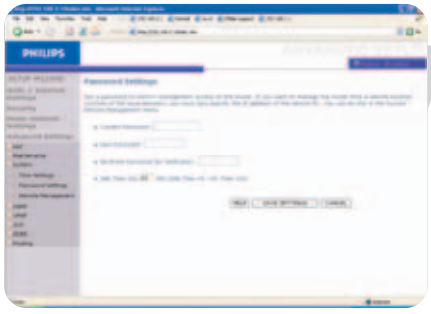
System



Time Settings
Select your local time zone from the drop down list. This information is used for log entries and client filtering.

For accurate timing of log entries and system events, you need to set the time zone. Select your time zone from the drop down list.

If you want to automatically synchronize the Wireless Router with a public time server, check the box to Enable Automatic Time Server Maintenance. Select the desired servers from the drop down menu.



Password Settings
Use this page to change the password for accessing the management interface of the Wireless Router.

Passwords can contain from 3~12 alphanumeric characters and are case sensitive.

Note: *If you lost the password, or you cannot gain access to the user interface, press the reset button on the rear panel, holding it down for at least five seconds to restore the factory defaults. By default, there is no password to login to the user interface.*

WARNING!
When you reset the Wireless Router using the blue reset button all configuration settings will be lost, also your ISP settings.

Enter a maximum Idle Time Out (in minutes) to define a maximum period of time for which the login session is maintained during inactivity.
If the connection is inactive for longer than the maximum idle time,
it will perform system logout, and you have to log in again to access the management interface. (Default: 10 minutes)

Remote Management
By default, management access is only available to users on your local network. However, you can also manage the Wireless Router from a remote host by entering the IP address of a remote computer on this screen. Check the Enabled check box, and enter the IP address of the Host Address and click 'SAVE SETTINGS'.

Note: *If you check Enable and specify an IP address of 0.0.0.0, any remote host can manage the Wireless Router.*

For remote management via WAN IP address you need to connect using port 8080. Simply enter WAN IP address followed by :8080, for example, 212.120.68.20:8080.

SNMP
Use the SNMP configuration screen to display and modify parameters for the Simple Network Management Protocol (SNMP).

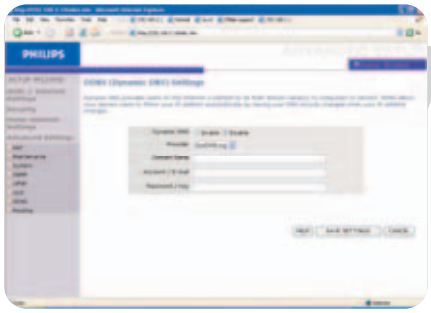
SNMP Community
A computer attached to the network, called a Network Management Station (NMS), can be used to access this information. Access rights to the agent are controlled by community strings. To communicate with the Wireless Router, the NMS must first submit a valid community string for authentication.

Parameter	**Description**
Community	A community name authorized for management access.
Access	Management access is restricted to Read Only (Read) or Read/Write (Write).
Valid	Enables/disables the entry.

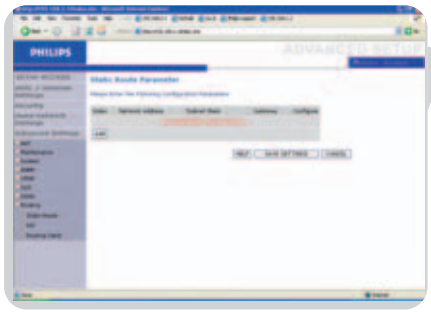
Note: Up to five community names may be entered.

SNMP Trap
Specify the IP address of the NMS to notify when a significant event is detected by the agent. When a trap condition occurs, the SNMP agent sends an SNMP trap message to any NMS specified as a trap receiver.

UPNP (Universal Plug and Play) settings
With Universal Plug and Play, a device can automatically dynamically join a network, obtain an IP address, communicate its capabilities, and learn about the presence and capabilities of other devices. Devices can then directly communicate with each other. This further enables peer-to-peer networking



DDNS (Dynamic DNS) settings
DDNS text 'Domain Name' is a series of alphanumeric strings separated by periods that maps to the address of a network connection and identifies the owner of the address.
Dynamic DNS provides users on the Internet with a method to tie their domain name to a computer or server. DDNS allows your domain name to follow your IP address automatically by having your DNS records changed when your IP address changes.
The Server Configuration section automatically opens the TCP port options checked in the Virtual Server section. Simply enter in the IP Address of your server, such as a web server, and then click on the port option HTTP Port 80 so users can access your web server from the Internet connection.
This DNS feature is powered by a DDNS service provider. With a DDNS connection you can host your own web site, email server, FTP site, and more at your own location even if you have a dynamic IP address. (Default: Disable)

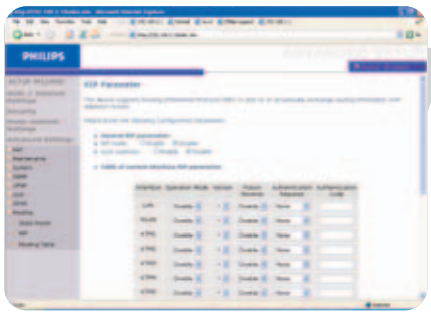


Routing
These pages define routing related parameters, including static routes and RIP (Routing Information Protocol) parameters.

Static route parameter

1 Click 'Add' to add a new static route to the list.

2 Click 'Save Settings' to save the configuration.



RIP parameter

RIP sends routing-update messages at regular intervals and when the network topology changes. When a router receives a routing update that includes changes to an entry, it updates its routing table to reflect the new route. RIP routers maintain only the best route to a destination.

After updating its routing table, the router immediately begins transmitting routing updates to inform other network routers of the change.

Routing table

After completing hardware setup by connecting all your network devices, you need to configure your computer to connect to the Wireless Router.
See: 'Windows 2000'
'Windows XP'
'Wireless adapters'

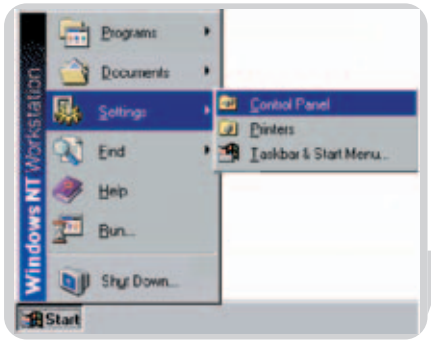
TCP/IP Configuration

To access the Internet through the Wireless Router, you must configure the network settings of the computers on your LAN to use the same IP subnet as the Wireless Router. The default IP settings for the Wireless Router are:

IP Address	192.168.1.2
Subnet Mask	255.255.255.0
DHCP function	Enable
DHCP IP Pool Range	192.168.1.11 to 192.168.1.60

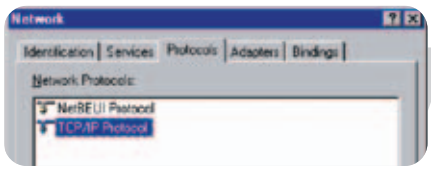
Note: *These settings can be changed to fit your network requirements, but you must first configure at least one computer to access the Wireless Router's web configuration interface in order to make the required changes. (See 'Configuring the Wireless Router' for instruction on configuring the Wireless Router.)*

Windows NT 4.0

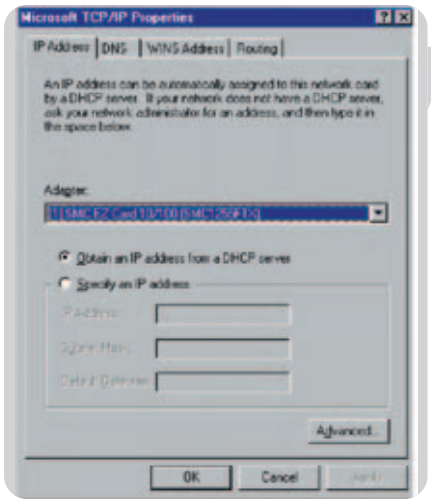


1 On the Windows desktop, click Start/Settings/Control Panel.

2 Double-click the Network icon.



3 In the Network window, select the Protocols tab.
Double-click TCP/IP Protocol.



4 When the Microsoft TCP/IP Properties window opens, select the IP Address tab.

5 In the Adapter drop-down list, make sure your Ethernet adapter is selected.

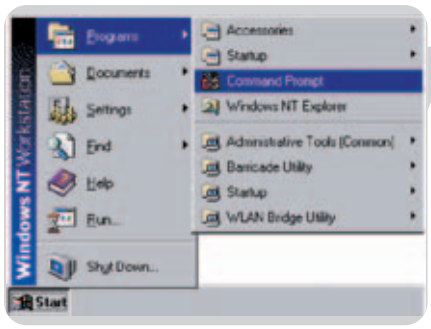
6 If 'Obtain an IP address automatically' is already selected, your computer is already configured for DHCP. If not, select this option and click 'Apply.'

7 Click the DNS tab to see the primary and secondary DNS servers. Record these values, and then click 'Remove.' Click 'Apply', and then 'OK.'

8 Windows may copy some files, and will then prompt you to restart your system. Click Yes and your computer will shut down and restart.

Disable HTTP Proxy
You need to verify that the 'HTTP Proxy' feature of your web browser is disabled. This is so that your browser can view the Wireless Router's HTML configuration pages (refer to 'Internet Explorer').

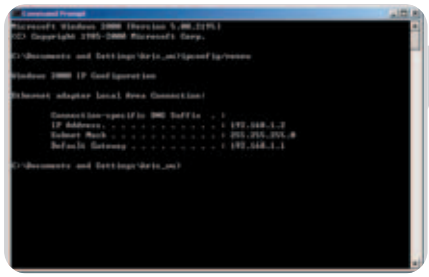
Obtain IP Settings from Your Wireless Router
Now that you have configured your computer to connect to your Wireless Router, it needs to obtain new network settings.
By releasing old DHCP IP settings and renewing them with settings from your Wireless Router, you will verify that you have configured your computer correctly.



1 On the Windows desktop, click Start/Programs/Command Prompt.

2 In the Command Prompt window, type 'IPCONFIG /RELEASE' and press the ENTER key.

3 Type 'IPCONFIG /RENEW' and press the ENTER key. Verify that your IP Address is now 192.168.1.xxx, your Subnet Mask is 255.255.255.0 and your Default Gateway is 192.168.1.2.
These values confirm that your Wireless Router is functioning.



4 Type 'EXIT' and press the ENTER key to close the Command Prompt window. Your computer is now configured to connect to the Wireless Router.

Windows 2000

1 On the Windows desktop, click Start/Settings/Network and Dial-Up Connections.

2 Click the icon that corresponds to the connection to your Wireless Router.

3 The connection status screen will open. Click Properties.

4 Double-click Internet Protocol (TCP/IP).

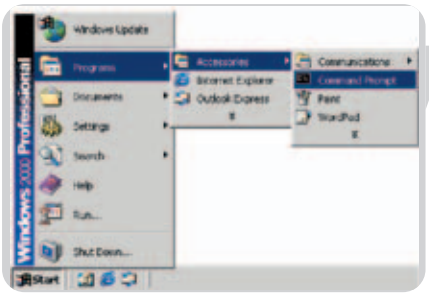
5 If 'Obtain an IP address automatically' and 'Obtain DNS server address automatically' are already selected, your computer is already configured for DHCP. If not, select this option.

Disable HTTP Proxy

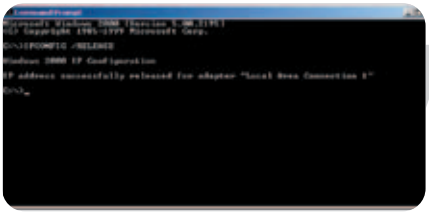
You need to verify that the 'HTTP Proxy' feature of your web browser is disabled. This is so that your browser can view the Wireless Router's HTML configuration pages (refer to 'Internet Explorer').

Obtain IP Settings from Your Wireless Router

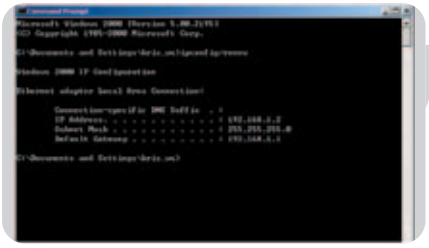
Now that you have configured your computer to connect to your Wireless Router, it needs to obtain new network settings. By releasing old DHCP IP settings and renewing them with settings from your Wireless Router, you can verify that you have configured your computer correctly.



1 On the Windows desktop, click Start/Programs/Accessories/Command Prompt.



2 In the Command Prompt window, type 'IPCONFIG /RELEASE' and press the ENTER key.



3 Type 'IPCONFIG /RENEW' and press the ENTER key. Verify that your IP Address is now 192.168.1.xxx, your Subnet Mask is 255.255.255.0 and your Default Gateway is 192.168.1.2.

These values confirm that your Wireless Router is functioning.

4 Type 'EXIT' and press the ENTER key to close the Command Prompt window.

Your computer is now configured to connect to the Wireless Router.

Windows XP

1 On the Windows desktop, click Start/Control Panel.

2 In the Control Panel window, click Network and Internet Connections.

3 The Network Connections window will open.
Double-click the connection for this device.

4 On the connection status screen, click Properties.

5 Double-click Internet Protocol (TCP/IP).

6 If 'Obtain an IP address automatically' and 'Obtain DNS server address automatically' are already selected, your computer is already configured for DHCP. If not, select this option.

Disable HTTP Proxy
You need to verify that the 'HTTP Proxy' feature of your web browser is disabled. This is so that your browser can view the Wireless Router's HTML configuration pages (refer to 'Internet Explorer').

Obtain IP Settings from Your Wireless Router
Now that you have configured your computer to connect to your Wireless Router, it needs to obtain new network settings. By releasing old DHCP IP settings and renewing them with settings from your Wireless Router, you can verify that you have configured your computer correctly.

1 On the Windows desktop, click Start/Programs/Accessories/Command Prompt.

2 In the Command Prompt window, type 'IPCONFIG /RELEASE' and press the ENTER key.

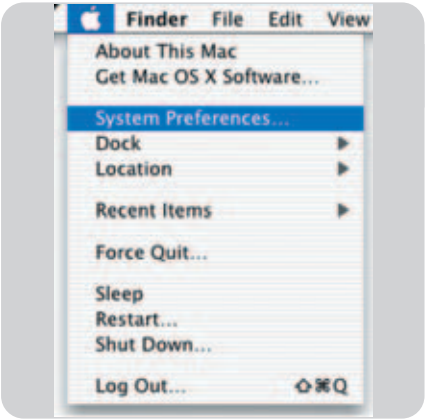
3 Type 'IPCONFIG /RENEW' and press the ENTER key. Verify that your IP Address is now 192.168.1.xxx, your Subnet Mask is 255.255.255.0 and your Default Gateway is 192.168.1.2. These values confirm that your Wireless Router is functioning.
Type 'EXIT' and press the ENTER key to close the Command Prompt window.

Your computer is now configured to connect to the Wireless Router.

Configuring Your Macintosh Computer

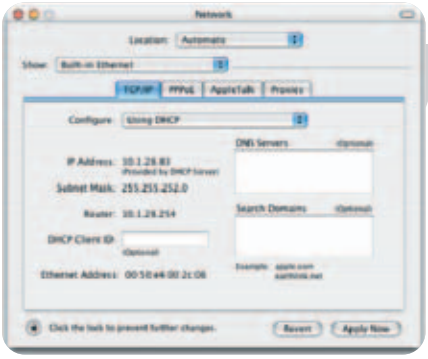
You may find that the instructions here do not exactly match your operating system. This is because these steps and screen shots were created using Mac OS 10.2. Mac OS 7.x and above are similar, but may not be identical to Mac OS 10.2.

Follow these instructions:



1 Pull down the Apple Menu. Click System Preferences.

2 Double-click the Network icon in the Systems Preferences window.



3 If 'Using DHCP Server' is already selected in the Configure field, your computer is already configured for DHCP. If not, select this Option.

4 Your new settings are shown on the TCP/IP tab. Verify that your IP Address is now 192.168.1.xxx, your Subnet Mask is 255.255.255.0 and your Default Gateway is 192.168.1.2. These values confirm that your Wireless Router is functioning.

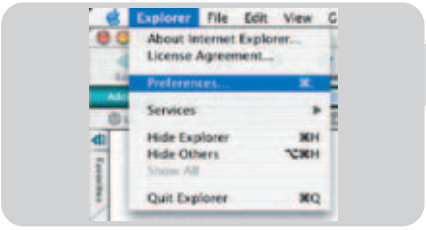
5 Close the Network window.

Now your computer is configured to connect to the Wireless Router.

Disable HTTP Proxy

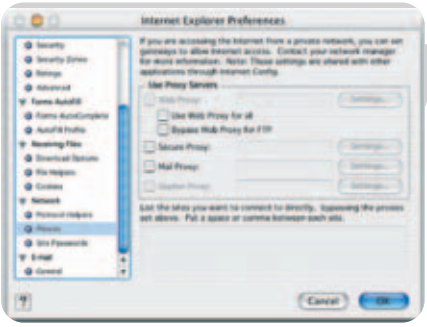
You need to verify that the 'HTTP Proxy' feature of your web browser is disabled. This is so that your browser can view the Wireless Router's HTML configuration pages. The following steps are for Internet Explorer.

Internet Explorer



1 Open Internet Explorer and click the Stop button.
Click Explorer/Preferences.

2 In the Internet Explorer Preferences window, under Network, select Proxies.



3 Uncheck all check boxes and click OK.

Configuring your wireless adapter

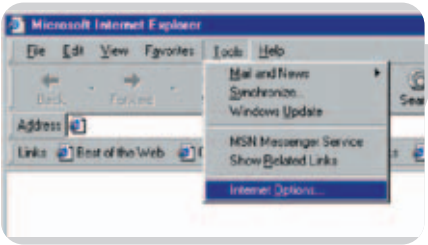
You can make a wireless connection with the SNB6500 using a Wi-Fi wireless adapter. Please read the manual of your Wi-Fi wireless adapter on how to connect to the SNB6500.

Disable HTTP Proxy

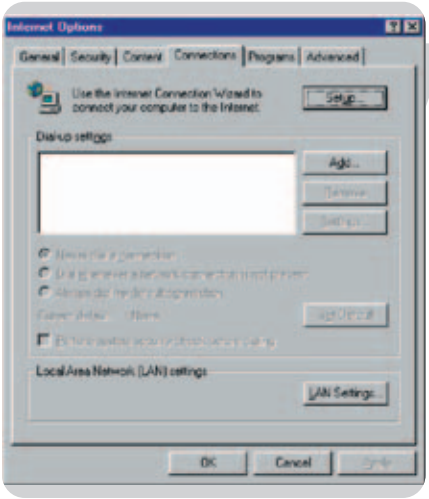
You need to verify that the 'HTTP Proxy' feature of your web browser is disabled. This is so that your browser can view the Wireless Router's HTML configuration pages. The following steps are for Internet Explorer.

Internet Explorer

1 Open Internet Explorer.



2 Click the Stop button, then click Tools/Internet Options.



3 In the Internet Options window, click the Connections tab.
Next, click the LAN Settings... button.

Finding the MAC address of a Network Card

MAC address

The MAC address can be used to prevent unwanted access to your Wireless Router. How to do this is explained in MAC Filter.
The MAC address has the format of xx:xx:xx:xx:xx:xx where x can be in the range of [0...9, A...F]

Windows NT4/2000/XP

Click Start/Programs/Command Prompt. Type 'ipconfig /all' and press 'ENTER'.

The MAC address is listed as the 'Physical Address.'

Macintosh

Click System Preferences/Network.

The MAC address is listed as the 'Ethernet Address' on the TCP/IP tab.

Linux

Run the command '/sbin/ifconfig.'

How to set-up a computer network?

The next pages will show you an example of how to set-up a computer network using the Philips Wireless Router.

Warning: The Wireless Router only establishes a connection between your wireless network devices. How you use this connection is up to you.

Setting-up a computer network is to be seen as an independent application that requires networking software from other manufacturers.
For example, the networking software that has been incorporated in the Windows Operating System by Microsoft.

Therefore, the description below is to be seen as an example only.

WHAT IS YOUR WINDOWS VERSION?

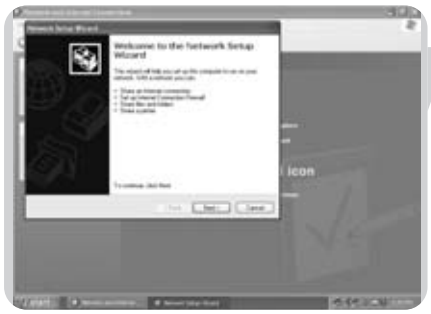
1. Start setting-up your network with the computer that has the latest operating system. The order of preference being: Windows XP, Windows 2000 , Windows ME and finally Windows 98SE.
2. Use its Networking Setup Wizard and allow it to make a networking setup diskette.
3. With this diskette, set-up your remaining computers.

For Windows XP and Windows 2000.
See further on in this chapter for Windows ME and Windows 98SE.

Click the Windows Start button, and click 'Control Panel' from the list.

Double-click the ‘Network and Internet connections’ icon.

Click in the list to the left on ‘Setting-up a home network or small business network’.



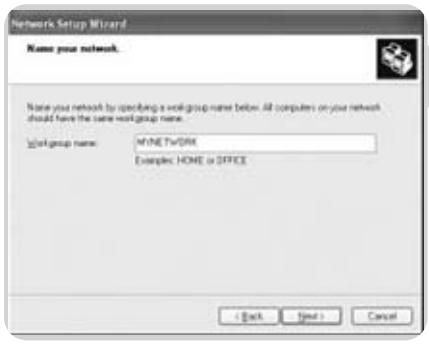
The Wizard Network Setup appears. Click ‘Next’ to continue.

Wizard Network Settings

1. Please, carefully read the instructions the Wizard gives you, and adapt your choices to the type of network you want to set-up. Use the Help feature within the Wizard if you need more information while using the Wizard.
2. In each window, click ‘Next’ to go to the next step.
3. Below, we will describe some of the crucial steps of this Wizard.

Place a check mark to ignore any broken network connections before clicking ‘Next’ to continue.

1. Enter a description that helps you recognize the computer.
2. Enter a name that is different for each computer.
3. Click ‘Next’ to continue.



Enter the same workgroup name for all computers in the network, then click ‘Next’ to continue.

Choose to make a networking setup disk. Then click ‘Next’.

Click ‘Finish’ to close the Wizard, and then use the disk you made to set-up your other computers.

To share folders with the network: Start Windows Explorer and right-click the folder you wish to share with the network. Click the ‘Sharing’ tab and adapt the settings.

To explore the network: Double-click the Network Environment icon on the desktop.
If you need more information, consult Windows Help.

For Windows ME and Windows 98SE.
See earlier on in this chapter for Windows XP and Windows 2000.

Click the Windows Start button, click 'Settings', and click 'Control Panel' from the list.

Double-click the 'Network' icon.

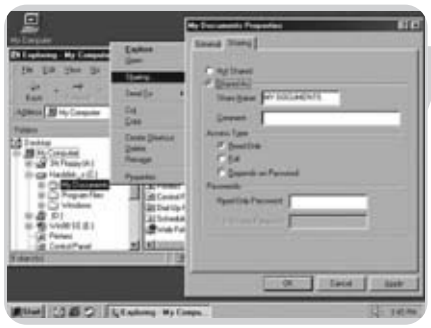
Click the 'Identification' tab.

1. Enter a name that is different for each computer.
2. Enter the same workgroup name for all computers in the network.
3. Enter a description that helps you recognize the computer.
4. Click on the 'Configuration' tab to continue.

Click the 'Sharing files and printers' button.

Select the access options you want, and click 'OK' to continue.

Click 'OK' to accept the changes.



To share folders with the network: Start Windows Explorer and right-click the folder you wish to share with the network. Click the 'Sharing' tab and adapt the settings.

To explore the network: Double-click the Network Environment icon on the desktop.
If you need more information, consult Windows Help.

Troubleshooting

This section describes common problems you may encounter and possible solutions to them. The Wireless Router can be easily monitored through panel indicators to identify problems.

Problem	**Cause/Solution**
I cannot browse to my Wireless Router	Your PC did not get an IP address from the Wireless Router. • Verify that your PC has an IP address. Open a command box (Windows key 'r', type cmd, hit enter). Type **ipconfig**. Check that your gateway address is 192.168.1.2 Your PC can not communicate with your Wireless Router. • Verify that you can communicate with the Wireless Router. Open a command box. Type ping 192.168.1.2 Response should be 'Reply from 192.168.1.2: bytes=32 time=110ms TTL=32' (time and TTL could be different)
My PC does not have/get an IP address	Network card is not configured to obtain an IP address automatically. • Check if Network Interface Card (NIC) is in DHCP mode. See chapter 'Configure your PC'. Network card speed does not match Wireless Router speed. • Set network adapter to a fixed speed on your computer. 1 Click **Start**. 2 Click **Settings**. 3 Click **Network Connections**. 4 Select you network card. Right mouse click. Select **Properties**. 5 Click Configure. 6 Click **Advanced** tab. Click Link Speed & Duplex. Select a **Full Duplex** speed (either 100Mbps or 10Mbps) Cable between PC and Wireless Router is not connected. • Check Ethernet cable and lights on the Wireless Router.

Glossary of terms

DHCP	Dynamic Host Configuration Protocol. This protocol automatically configures the TCP/IP settings of every computer on your home network.
DNS Server Address	DNS stands for Domain Name System, which allows Internet host computers to have a domain name and one or more IP addresses. A DNS server keeps a database of host computers and their respective domain names and IP addresses, so that when a domain name is requested, the user is sent to the proper IP address. The DNS server address used by the computers on your home network is the location of the DNS server your ISP has assigned.
DSL Modem	DSL stands for Digital Subscriber Line. A DSL modem uses your existing phone lines to transmit data at high speeds.
Ethernet	A standard for computer networks. Ethernet networks are connected by special cables and hubs, and move data around at up to 10 million bits per second (Mbps).
HPNA	Home Phone Line Networking Alliance, which is an association of corporations (including) working to ensure the adoption of a single, unified phone line networking standard. Your Home Connect home network gateway is compliant with HPNA Specification 2.0, which allows networking speeds of up to 1 million bits per second (Mbps) using your existing home phone lines.
IP Address	IP stands for Internet Protocol. An IP address consists of a series of four numbers separated by periods, that identifies an single, unique Internet computer host. Example: 192.34.45.8.
ISP Gateway Address (see ISP for definition)	The ISP Gateway Address is an IP address for the Internet router located at the ISP's office. This address is required only when using a cable or DSL modem.
ISP	Internet Service Provider. An ISP is a business that provides connectivity to the Internet for individuals and other businesses or organizations.
LAN	Local Area Network. A LAN is a group of computers and devices connected together in a relatively small area (such as a house or an office). Your home network is considered a LAN.
MAC Address	MAC stands for Media Access Control. A MAC address is the hardware address of a device connected to a network.
NAT	Network Address Translation. This process allows all of the computers on your home network to use one IP address. Using the NAT capability of the Home Connect home network gateway, you can access the Internet from any computer on your home network without having to purchase more IP addresses from your ISP.
PPPoE	Point-to-Point Protocol over Ethernet. Point-to-Point Protocol is a method of secure data transmission originally created for dial-up connections; PPPoE is for Ethernet connections.
RJ-45	Registered Jack-45, 8 wire connector
Secondary Dial-Up	A secondary dial-up phone number is used by your ISP in case your primary dial-up number has too many other customers accessing it. The secondary dial-up phone number will be used if your primary dial-up phone number cannot be accessed.
SPI	Stateful Packet Inspection. SPI is the type of corporate-grade Internet security provided by your Home Connect home network gateway. Using SPI, the gateway acts as a "firewall", protecting your network from computer hackers.
Subnet Mask	A subnet mask, which may be a part of the TCP/IP information provided by your ISP, is a set of four numbers configured like an IP address. It is used to create IP address numbers used only within a particular network (as opposed to valid IP address numbers recognized by the Internet, which must assigned by InterNIC).
TCP/IP	Transmission Control Protocol/Internet Protocol. This is the standard protocol for data transmission over the Internet.
WAN	Wide Area Network. A network that connects computers located in geographically separate areas, (i.e., different buildings, cities, countries). The Internet is a wide area network.

Physical Characteristics

Ports
– Four 10/100Mbps RJ-45 Ports

Management Features
– Firmware upgrade via web based management
– Web based management (configuration)
– Power indicators
– Event and history logging
– Network ping

Security Features
– Password protected configuration access
– User authentication (PAP/CHAP) with PPP
– Firewall NAT NAPT
– VPN pass through (IPSec-ESP Tunnel mode,L2TP, PPTP)

LAN Features
– IEEE 802.1d (self-learning transparent Bridging)
– DHCP Server
– DNS Proxy
– Static Routing, RIPv1 and RIP

Radio Features
– Wireless RF module Frequency Band
– 802.11g Radio: 2.4GHz
– 802.11b Radio: 2.4GHz
Europe - ETSI
– 2412~2472MHz (Ch1~Ch13)

Modulation Type
– OFDM, CCK

Operating Channels IEEE 802.11b compliant:
– 13 channels (ETSI)

Operating Channels IEEE 802.11g compliant:
– 13 channels (Europe)

RF Output Power Modulation Rate-Output Power (dBm)
802.11b - 1Mbps (16 dBm)
802.11b - 2Mbps (16 dBm)
802.11b - 5.5Mbps (16 dBm)
802.11b - 11Mbps (16 dBm)

Modulation Rate-Output Power (dBm)
802.11g - 6Mbps (15 dBm)
802.11g - 9Mbps (15 dBm)
802.11g - 12Mbps (15 dBm)
802.11g - 18Mbps (15 dBm)
802.11g- 24Mbps (15 dBm)
802.11g - 36Mbps (15 dBm)
802.11g- 48Mbps (15 dBm)
802.11g - 54Mbps (15 dBm)
802.11g - 108Mbps (15 dBm)

PHILIPS

AQ95-56F-611KR
(report No.)

EC DECLARATION OF CONFORMITY

We , Philips Consumer Electronics B.V., P&A CC: Building SBP6
(manufacturer's name)

P.O.Box 80002, 5600 JB Eindhoven, The Netherlands
(manufacturer's address)

declare under our responsibility that the electrical product:

Philips
(name)

SNB6500 -/00 -/05
(type or model)

Wireless Base Station 11 b/g
(product description)

to which this declaration relates is in conformity with the following standards:

EN 300 328 v1.6.1 (2004-11)
EN 301 489-1 v1.4.1 (2002-08)
EN 301 489-17 v1.2.1 (2002-08)
EN60950-1 :2001
EN60950:2000
(title and/or number and date of issue of the standards)

following the provisions of 1999/5/EC (R&TTE Directive)
and is produced by a manufacturing organisation on ISO 9000 level.

Eindhoven, 16/06/2005
(place, date)

K.Rysman
Approbation manager
(signature, name and function)

Guarantee certificate
Certificat de garantie
Garantieschein
Garantiebewijs
Certificado de garantia
Certificato di garanzia
Certificado de garantia
Εγγύηση
Garantibevis
Garanticertifikat
Garantibevis
Takuutodistus

year warranty
année garantie
Jahr Garantie
jaar garantie
año garantia
anno garanzia
χρόνος εγγύηση
år garanti
år garanti
år garanti
vuosi takuu
año garantia

Type: **SNB6500**

Serial nr: _____

Date of purchase - Date de la vente - Verkaufsdatum - Aankoopdatum - Fecha de compra - Date d'acquisito - Data da adquirição - Ημερομηνία αγοράς - Inköpsdatum - Anskaffelsesdato - Kjøpedato - Oatopäivä -

Dealer's name, address and signature
Nom, adresse et signature du revendeur
Name, Anschrift und Unterschrift des Händlers
Naam, adres en handtekening v.d. handelaar
Nombre, direccion y firma del distribudor
Nome, indirizzo e firma del fornitore
Ονοματεπώνυμο, διεύθυνση και υπογραφη του εμπ. προμηθευτη
Återförsäljarens namn, adress och signatur
Forhandlerens navn, adresse og unterskrift
Forhandlerens navn, adresse og unterskrift
Jälleenmyyjän nimi, osoite ja allekirjoitus
Nome, morada e assinature da loja

CE 0682

Specifications are subject to change without notice.
Trademarks are the property of Koninklijke Philips Electronics N.V. or their respective owners.
2006 © Koninklijke Philips Electronics N.V. All rights reserved.

www.philips.com

DFU-SNB6500-ENG-V2.0